Integrating CDX into the Graduate Program[*]

Gregg H. Gunsch, Richard A. Raines, and Timothy H. Lacey
Department of Electrical and Computer Engineering
Graduate School of Engineering and Management
Air Force Institute of Technology, Wright-Patterson AFB, OH 45433-7765
{Gregg.Gunsch, Richard.Raines, Timothy.Lacey}@afit.edu

Abstract – *The Air Force Institute of Technology competed for the first time in the all-service Cyber Defense Exercise this year. To do so required a restructuring of the existing specialty track in information systems security/assurance, in order to align with the exercise schedule and maintain an appropriate graduate-level emphasis. In addition, the school was able to enroll, for the first time ever, senior enlisted members of the Air Force and Marine Corps who contributed a wealth of tactical, practical, knowledge and experience in deploying information systems under less than ideal conditions. The merits of these factors were borne out by the school's success on its maiden effort.*

Keywords: Computer security, network security, computer defense, cyberdefense, Cyber Defense Exercise.

1 Introduction

When the Cyber Defense Exercise (CDX) was first initiated in 2001, the graduate school of the Air Force Institute of Technology (AFIT) was not in a good position to participate and hold much hope of being a credible player. The timing of the exercise with respect to the upper- and under-class students' programs could hardly be worse. Over time however, as AFIT cemented its position as a leader in information assurance education and the CDX grew in extent and popularity, it became increasingly clear that regardless of the hurdles, AFIT's participation would become an achievable and agreeable imperative. Through creative restructuring of the existing educational paths, and invigorated institutional support, AFIT was able to effect a strong entry and win the graduate school competition of the CDX (CDX-PG) on its first foray.

2 The AFIT Master's Program

The historically typical AFIT in-residence graduate program requires a junior Air Force officer to work full-time to achieve a master's degree, with thesis, over a course of nineteen months. Each year roughly two hundred students arrive in late August, with a target graduation date of March, two years hence. Each program consists of a nominal 60 quarter credit hours of course work and 12 credit hours of independent research (oral defense and written thesis) as the educational capstone. Most programs require a core component of courses consistent with the student's chosen or assigned degree, then provide an opportunity to specialize in an aspect related to that discipline. In 1996, AFIT developed a specialized sequence of courses in Information Systems Security/Assurance (ISSA), targeted specifically for students in the graduate computer science/systems (GCS) and computer engineering (GCE) programs.

2.1 Winds of Change

While the number of GCS/GCE students who were interested in ISSA steadily grew, it was not until 1999 before the course enrollment leaped beyond expectations. In 1999 the two graduate schools of AFIT, one business and one engineering, were merged to become the Graduate School of Engineering and Management. The ISSA specialization quickly became a popular component of the graduate information resource management (GIR) and information systems management (GIS) programs, effectively doubling the class size and infusing a whole new challenge for the instructor. It was then paramount that he simultaneously embrace and integrate the managerial and technological aspects of ISSA, providing appropriate emphasis on both. This approach afforded the management students a much richer exposure to technology than they would otherwise experience, and it forced the technologists to address weightier issues and grapple with a much larger "big picture" than technical solutions could offer. The first offerings of this more integrated approach were "rocky" at best, but the inclusion of the CDX promised to provide a unifying framework.

While officers from other services have had access to AFIT's graduate programs, for the first time ever, enlisted members have the opportunity to pursue ad-

[*] **The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government. U.S. Government work is not protected by U.S.copyright.**

vanced degrees with the sponsorship of their services. Over a dozen senior enlisted Air Force and Marine Corps members are currently enrolled in AFIT graduate programs. Seven of them have declared ISSA as their educational specialty.

In March 2002, AFIT was formally designated by the NSA as a national Center of Academic Excellence in Information Assurance Education. This recognition was leveraged into institutional and infrastructural support for the founding of AFIT's Center for INFOSEC Education and Research (CIER), established as the focal point of AFIT's ISSA efforts and the vehicle with which to cultivate funding sources. It was the achievement of this "critical mass" that allowed serious consideration of the effort, investment and curriculum restructuring necessary to support the Cyber Defense Exercise.

2.2 Modifying the Curriculum

The greatest hindrance to AFIT's involvement in the CDX was timing: the fact that the exercise occurs early in the Spring quarter. This places the CDX several weeks after graduation of the upper-class, and early in the third quarter of the under-class programs. While many graduating students would have volunteered to be placed on casual status after graduation in order to participate in the exercise, the huge amount of pre-exercise preparations would have seriously jeopardized their ability to complete their theses on time and with the requisite quality. Hence, the responsibility for conducting the CDX fell upon the under-class, with pre-exercise preparations occurring throughout the second quarter of their program. Ideally, for AFIT students, the CDX should occur four months later.

The typical specialty sequence is a series of three courses, each building upon the previous. They also build upon the foundational knowledge provided by the degree core courses. For that reason, they tend to follow a winter-spring-summer pattern, allowing the students to use the first (fall) quarter to complete foundational and prerequisite courses. ISSA was no exception.

The first course in the ISSA sequence was CSCE525, Introduction to Information Warfare. It provided a broad overview of the whole of information warfare/operations, from a historical perspective through the information age, covering classic and modern doctrine, and inculcating the students with an appreciation of what information assurance means to the warfighter. Its main purpose was to persuade the students to view the other two ISSA courses not as computer security, but rather as relating to the deployment and protection of mission-essential weapons systems. These two courses, CSCE625 and CSCE725 (Information Systems Security, Assurance and Analysis I and II, respectively), provide the technical and managerial content for achieving ISSA. In concert with the original timing of the ISSA sequence, many students would also be taking complementary courses in computer architecture, communication networks, distributed software and operating systems, and cryptography.

To accommodate the CDX, CSCE625 was moved forward to the Winter quarter for pre-exercise preparations. CSCE725 was moved to the Spring, where the first two weeks were spent in eleventh-hour hardening and vulnerability testing. The subject matter was reorganized between the courses so that only those topics germane to the CDX would be covered in CSCE625; for example, firewalls, viruses, forensics and data hiding were deferred until after the CDX. Material from other courses, such as communication networks, had to be introduced early to be of use. The perspective-setting course, CSCE525, was postponed until the Summer quarter due to scheduling constraints. This was not an ideal situation for a smooth academic flow. The students concurred, with comments like "the material feels out of order" and "this course (CSCE625) is too early in my program." The end-of-course critiques of CSCE625 were very diverse, with some students harshly criticizing the sense of incompleteness, and others enjoying what they learned but deferring judgment until after the CDX.

While the CDX disrupted the existing program, it added a whole new dimension of rich educational experience to the ISSA curriculum. It energized the students' self-directed learning, and left them with a strong sense of satisfaction and accomplishment.

3 CDX2003

Twenty-seven students populated CSCE625: too many to effectively manage alone. The instructor selected three students to operate as *Team 1*, the AFIT CDX Network Command team, based on observed leadership abilities and background. These were Capt Joshua Green (electrical/computer engineering), Capt Michael Hass (information resource management), and USMC GySgt Brian Hamilton (information resource management). Team 1 was responsible for the complete conduct of the exercise. They dissected the requirements of the OpOrd and assigned teams to tasks and students to teams, then reconstituted the assignments as necessary throughout the course of the exercise (not all students remained for CSCE725, and not all tasks were necessary to continue once the exercise began). During the CDX they gathered daily situation reports from the other teams to compile for submission to CDX/HQ, developed a rotating shift schedule, and ensured that all functions were kept operational.

The instructor's involvement during the pre-exercise phase was minimal, and practically non-existent during the exercise. He worked with Team 1 to understand the requirements of the OpOrd and to establish an operating baseline: Windows 2000 Professional was to be the operating system of choice across the servers, and IPSec was to be utilized everywhere possible. The students were responsible to lock down the Windows configuration, using the NSA Security Recommendation Guides (http://nsa1.www.conxion.com/win2k/index.html) as a baseline. The student teams determined what else was required to provide the requisite functionality demanded by the OpOrd.

3.1 Integration into the Courses

Since the pre-exercise preparations were integrated into CSCE625, student deliverables were necessary for instructor evaluation. The student teams were required to research and formally report to the class on a series of questions:

- What do you need to do to achieve your assigned functionality?
- What are the alternatives?
- Why did you select your solution?
- How does it integrate with the other functions?
- What other functions do you depend on, and what depends on you?
- What vulnerabilities does your solution have, and how are they exploited?
- What will you do to prevent exploitation of your solution?
- How will your preventative measures effect the other functions?
- What will you monitor?
- How will you analyze your data?
- How will you know you are successful?
- What backup systems and procedures do you require? How often will you back up data?
- What is your plan for recovery/reconstitution?
- How will you test it?

This process was repeated throughout the quarter in order to expedite integration among teams, and to educate the other students on the tradeoffs being made regarding design decisions.

After a short spring break, the students spent the first two weeks of CSCE725 finishing the integration of the functions and performing vulnerability/penetration testing. A number of last-minute problems were worked out, then each team practiced their documented recovery procedures. Team 1 ensured that each member of the function teams was capable of tearing down and rebuilding that particular function. Reconstitution of the function teams was also accomplished as necessary, moving people to augment the teams appropriately. Some overlap was also developed, so that often at least one person "on watch" was capable of supporting multiple functions.

The exercise itself was generally uneventful. For the most part, the systems withstood the Red Team onslaughts. The students did neglect to secure a switch, discounting it as something outside the scope of the Red Team's target set (even though it was discussed early on in CSCE625 as a concern). After a rather blatant commandeering of that switch by the Red Team, the students identified the problem and replaced the switch with a spare, then locked down the new switch so that it was invisible to the outside world. It did take some effort to put the original switch back into service, and the demerits earned by this oversight were well deserved.

Camaraderie was high during the exercise, enhanced greatly by the presence of enlisted Marines who provided additional physical security and maybe enjoyed just a bit too much the opportunities to challenge "noncombatants" attempting to enter the lab. For the most part, the exercise simulated the real world with very high fidelity: long periods of absolute boredom, punctuated by brief flurries of activity.

After the exercise, the student performed a reasonable amount of post-mortem analysis and reflection, documenting those results and suggestions for future exercises in a set of after-action reports. We had hoped that the Red Team and White Cell would have been able to provide additional information, in particular regarding exploit attempts and accomplishments that we may have overlooked, but they were overcome by real-world events and were unable to follow through. We hope and advise that such out-briefings be given high priority and the necessary resources in future exercises: we believe they can add significantly to the learning experience.

The remainder of CSCE725 was spent catching up on deferred topics, such as identity theft, wireless systems, viruses and Trojan horses, and participating in hands-on labs such as virus creation and computer forensic exercises.

3.2 Star Player Awards

The students responded to a poll to nominate their peers who contributed the most to AFIT's success in the CDX and in helping to educate their fellow students. Three students stood out well above the rest:

- MSgt Brad Kuntzelman, for the enormous wealth of knowledge and experience he provided across most of the required areas of functionalty, but in particular, his dogged determination and capability to keep the Exchange Server fully operational
- Capt Danny Bias, for his team leadership abilities and expertise in keeping the Web Server operational even under high attack
- GySgt Juan Lopez, who researched and practically single-handedly designed and monitored the network intrusion detection architecture

Each of these students were publicly presented with a framed memento of their contributions. The students also gave special thanks and recognition to our Information Assurance Lab Administrator, Mr. Tim Lacey, for his tremendous efforts, talents and tireless support of the exercise.

3.3 Primary After-Action Report Issues

The consensus among the teams was that this exercise had several constraints (e.g., must use this database) and non-realistic configurations (e.g., no host-based firewalls allowed) that made the exercise less than plausible. In addition, expectations were high and desired that the Red Teams would be able to rip through our systems, taking things down at will so we would be severely challenged to respond and recover. As it was, with limited CDX and Red Team resources, and the inherent strengths of properly configured software, the exercise primarily consisted of demonstrating that we could deflect most onslaughts without serious degradation of functionality.

Although it seemed a reasonable solution at the beginning, the choice to use Exchange Server (5.5, then later 2000) turned out to be overkill. A lot of unnecessary (according to the OpOrd) functionally was provided, which only added to the complexity and vulnerability of the system, and caused several service outages not even initiated by the Red Team.

4 Recommendations

The students compiled a set of recommendations regarding exercise scenario construction in future exercises. These are provided herein without modification or comment.

1. Exercise Day Zero

   (a) Functionality Test: Some 4-hour block to establish that all appropriate services are functioning and that initial capability list are properly established (whether secured or not). This would basically be a "functional assessment" day to ensure basic services are available. Any needed IP addresses could be exchanged, etc. No points assessed during this phase.

2. Exercise Day One

   (a) Red Team Vulnerability Assessment

      i. For first 4-hours (or whatever is appropriate) the Red Team performs all the scans it requires to assess the vulnerabilities of the network. It's envisioned that this is a one shot opportunity to scan. Some debate on whether or not the Red Team should be able to place backdoors during this phase.

      ii. During this session the Blue Team is not allowed to observe (virtually, directly, indirectly, etc) any of the Red Team activities, to include passive monitoring/recording.

      iii. From this initial monitoring a (unrevealed) score should be provided on how well the Blue Team secured its network while providing expected service.

   (b) Red Team Contrived Scenarios - Unobserved by Blue Team

      i. Red Team uses some subset of identified vulnerabilities and performs some misuse of the system which the Blue Team may NOT observe. Blue Team must be allowed *some* normal level of logging, but not complete "ethereal-like" recording of traffic.

      ii. The Blue Team must find the damage, assess the impact, undo it if possible, and restore services. Blue Team may make NO OTHER security changes during this phase (i.e. block other holes that are stumbled across, although it is reasonable to assume some patching will fix multiple holes).

      iii. Some scoring should occur based on how well the hack was identified, its ability to restore to the original environment (bonus points for continuing to provide service to legitimate users), and its ability to patch the vulnerability (if possible).

      iv. If necessary, at some time interval, the Red Team may reveal additional hints as to where damage lies.

      v. Red Team should perform a follow-up "misuse" to verify vulnerability was appropriately blocked (if possible).

3. Exercise Day Two

   (a) Red Team Contrived Scenarios - Observed by Blue Team

      i. Red Team uses some subset of identified vulnerabilities and performs some misuse of the system which the Blue Team may actively observe through any possible means, but NOT act.

      ii. Similar to the unobserved scenarios, the Blue Team must find the damage, assess it, undo it, restore services, etc. Points assessed appropriately. Red Team does follow-up as appropriate. Similar to above, Blue Team must restrict its changes to the vulnerability only.

   (b) Red Team Assault - Blue Team Active Defense

      i. Red Team uses remaining identified vulnerabilities and executes direct assault on some/all of those vulnerabilities as it sees fit.

ii. Blue Team may actively defend the network using legitimate actions (clearly defined) based on observed events.

iii. Severe penalties should be levied against any action which denies service against “real” user traffic or that “blocks” IPs indiscriminately without real cause (i.e. Blue Team blocking an IP simply because it pinged a box is NOT a good cause for blocking). Blue Team’s thresholds for blocking should be defined in their CONOPS, as well as the actions that will occur when misuse occurs.

iv. Points should be awarded based on ability to maintain service to legitimate users (e.g. disconnecting a server as a solution should result in minimal points; killing an offending process and blocking the offending IP across the domain results in maximal points; etc.)

4. Much of this is conceptually based on the Red Team discovering some useful set of vulnerabilities with their initial scans. If it is believed that the number of vulnerabilities will not be of useful quantity, we recommend the Red Team pre-configure servers identically across the schools. The CDX could then have a few days of unobserved and observed scenarios (as above), perhaps a week or two of downtime where Blue Team can lockdown the device, then a continuance (either as above or some subset thereof).

5 Conclusions

The students learned an enormous amount in preparing for the exercise, so the CDX proved itself to be a valuable and enjoyable component of the ISSA track. The students were able to immerse themselves in the application of security engineering techniques as they were being taught. AFIT definitely intends to compete in subsequent exercises, building upon the lessons learned from this year’s competition.

The closing comments of Team 1’s final After Action report says it all: “CDX is far from an easy exercise. It requires a great deal of planning, followed by lengthy and often meticulous work, followed by an exercise which is both long and difficult. However, the hands-on approach helped bridge the gap between class lecture and the real world. Being able to apply recently learned theory, rules and guidelines to an actual network expands the knowledge of the students exponentially. With a well thought-out strategy and proper execution, it is possible to keep even the best hackers from NSA and AFIWC at bay.”

6 Acknowledgments

We would like to recognize the students for the outstanding job they did on CDX2003:

Capt Danny R. Bias, USAF
1stLt Jeffrey A. Boggs, USAF
1stLt Richard D. Booker, USAF
GySgt Pamela J. Cole, USMC
MSgt Charlie I. Cruz, USAF
1stLt Matthew D. Eyster, USAF
Capt David C. Fitzgerald, USAF
Capt Joshua D. Green, USAF
GySgt Brian K. Hamilton, USMC
Capt Michael C. Hass, USAF
2dLt Michael J. Henson, USAF
1stLt Peter L Hinrichsen, USAF
2dLt Terence D. Hunt, USAF
1stLt Mary M. King, USAF
MSgt Brad Kuntzelman, USAF
GySgt Juan Lopez, USMC
1stLt Brent T. Mcbride, USAF
Capt Jachin Sakamoto, USAF
GySgt Kelvin B. Scott, USMC
MSgt Duane C. Sorgaard, USAF
1stLt Eugene D. Turnbaugh, USAF
1stLt Neal A. Watts, USAF